JOURNAL OF NUMBER THEORY 36, 80–84 (1990)

A Generalization of Ehrenfeucht's Irreducibility Criterion

G. ANGERMÜLLER

Mathematisches Institut der Universität Erlangen-Nürnberg, Bismarckstr. 1½, D-8520 Erlangen, West Germany

Communicated by H. L. Montgomery

Received June 1, 1985

For polynomials of the form $Q = P(f(\mathbf{X}), g(\mathbf{Y}))$, where P is a generalized difference polynomial and f, g are polynomials in several variables, we prove a sufficient criterion for irreducibility. Moreover, we show that (in characteristic 0) any two non-constant factors of Q cannot generate the unit ideal in the polynomial ring with variables $\mathbf{X}, \mathbf{Y}$. © 1990 Academic Press, Inc.

Let k be a field of characteristic $p \geqslant 0$ and $\mathbf{X} = X_1, \ldots, X_m$, $\mathbf{Y} = Y_1, \ldots, Y_n$ be independent systems of variables over k. Recall [1, 4] that a *generalized difference polynomial of type* (d, e) is a polynomial

$$P(U, V) = cU^e + \sum_{i=1}^{e} P_i(V)\, U^{e-i}$$

in two variables U, V such that $e > 0$, c is a non-zero constant, $d = \deg P_e(V) > 0$, and $\deg P_i(V) < di/e$ for $0 < i < e$. The aim of this note is to prove the following theorem and its corollaries:

THEOREM. *Let $P(U, V)$ be a generalized difference polynomial of type (d, e) and $f(\mathbf{X}) \in k[\mathbf{X}]$, $g(\mathbf{Y}) \in k[\mathbf{Y}]$; further, let $q(\mathbf{X}, \mathbf{Y}) = P(f(\mathbf{X}), g(\mathbf{Y}))$. Then we have:*

(a) *If $p \nmid de(\deg f)(\deg g)$ and $r, s \in k[\mathbf{X}, \mathbf{Y}]$ are non-constant factors of q, then $(r, s) \neq (1)$ in $k[\mathbf{X}, \mathbf{Y}]$. In particular, if k is algebraically closed, r and s have a common zero.*

(b) *If $\gcd(e \cdot \deg f, d \cdot \deg g) = 1$ then q is irreducible.*

Part (a) generalizes the main result from [1, 4], whereas part (b) extends Ehrenfeucht's criterion [2, 3, 6].

Let us state two important special cases in the corollaries.

COROLLARY 1. *Let $f(\mathbf{X}) \in k[\mathbf{X}]$, $g(\mathbf{Y}) \in k[\mathbf{Y}]$. Then we have:*

0022-314X/90 $3.00

(a) *If* $p \nmid (\deg f)(\deg g)$ *and* $r, s \in k[\mathbf{X}, \mathbf{Y}]$ *are non-constant factors of* $f(\mathbf{X}) + g(\mathbf{Y})$ *then* $(r, s) \neq (1)$ *in* $k[\mathbf{X}, \mathbf{Y}]$. *In particular, if* k *is algebraically closed,* r *and* s *have a common zero.*

(b) *If* $\gcd(\deg f, \deg g) = 1$ *then* $f(\mathbf{X}) + g(\mathbf{Y})$ *is irreducible.*

To obtain a proof of corollary 1, we only have to apply the theorem with $P(U, V) = U + V$.

COROLLARY 2. *Let* $P(U, V)$ *be a generalized difference polynomial of type* (d, e). *Then we have*:

(a) *If* $p \nmid de$ *and* r, s *are non-constant factors of* P *then* $(r, s) \neq (1)$ *in* $k[U, V]$. *In particular, if* k *is algebraically closed,* r *and* s *have a common zero.*

(b) *If* $\gcd(d, e) = 1$ *then* P *is irreducible.*

This is the special case $f = U$, $g = V$ of the theorem.

Remarks. (1) Let $p > 0$. The identity

$$U + U^p + V + V^p = (U + V)(1 + (U + V)^{p-1})$$

shows that in part (a) of the above corollaries the assumption on p cannot be omitted.

(2) Let k be an algebraically closed field. Under the assumptions of part (a) of the Theorem it follows that the zero-set of q is connected in the Zariski topology. If more specially, k is the complex number field, the zero-set is connected in the usual topology too; in fact, any Zariski-closed irreducible set is connected in the usual topology and trivially any union of pairwise intersecting connected sets is connected.

To prove the theorem, we shall use the following *notation*: For $0 \neq f \in k[\mathbf{X}]$ let $f = f_0 + \cdots + f_d$ with $f_d \neq 0$ be the decomposition of f in homogeneous polynomials f_i of degree i; f_d is called the *degree form* of f. We call f *squarefree*, if no square of a non-constant polynomial divides f.

We shall see that part (a) of the theorem is a special case of the following

PROPOSITION. *Let* $f \in k[\mathbf{X}]$ *be a polynomial with squarefree degree form. If* r, s *are non-constant factors of* f, *then* $(r, s) \neq 1$ *in* $k[\mathbf{X}]$; *in particular, if* k *is algebraically closed,* r *and* s *have a common zero.*

Proof. Observe that the additional remark is an immediate consequence of Hilbert's Nullstellsatz.

Replacing k by a simple transcendental extension of k we can assume that k has infinitely many elements. So we can find variables

$$U_1 = X_1,\ U_2 = X_2 + c_2 X_1,\ \ldots,\ U_m = X_m + c_m X_1$$

with $c_2, \ldots, c_m \in k$ suh that f is unitary in $U = U_1$ and $\deg_U f = \deg f$.

Now assume $(r, s) = (1)$ and choose $a, b \in k[\mathbf{X}]$ such that

$$ar + bs = 1. \tag{1}$$

To obtain a contradiction, we procceed as in the proof of Theorem (1) in [4]. Let R (resp. F) be the degree form of r (resp. f). From $r \mid f$ we conclude $R \mid F$ and so we see that r is a unitary polynomial in U such that

$$\deg r = \deg R = \deg_U R = \deg_U r. \tag{2}$$

Applying the Euclidean algorithm we obtain $c, d \in k[\mathbf{X}]$ such that

$$b = cr + d,\ \deg_U d < \deg_U r. \tag{3}$$

Inserting (3) in (1) we obtain the relation

$$(a + cs)r + ds = 1. \tag{4}$$

Now let D (resp. S) be the degree form of d (resp. s). By (4) we have $d \neq 0$ and $R \mid DS$. Further, by (2), (3) we obtain

$$\deg_U D \leqslant \deg_U d < \deg_U r = \deg_U R$$

and thus a non-constant factor of R has to divide S. This implies that F is not squarefree, a contradiction. So our hypothesis is false, i.e., $(r, s) \neq (1)$.

COROLLARY. *Let $f \in k[\mathbf{X}]$ be a polynomial with squarefree degree form and such that $(f, \partial f/\partial X_1, \ldots, \partial f/\partial X_m) = (1)$. Then f is absolutely irreducible.*

Proof. Obviously we can assume k algebraically closed. If f could be written as $f = rs$ with non-constant r, s there would be a common zero of r and s by the proposition; but such a zero is a common zero of $f, \partial f/\partial X_1, \ldots, \partial f/\partial X_m$, contradicting the assumption. This shows that f is irreducible.

Proof of the Theorem. (a) As in the proof of the proposition we can assume that f (resp. g) is unitary in $U = X_1$ (resp. $V = Y_1$) and $u = \deg f = \deg_U f$, $v = \deg g = \deg_V g$.

Now assume $(r, s) = (1)$. Then

$$r' = r(X_1^{dv}, X_2, \ldots, X_m, Y_1^{eu}, Y_2, \ldots, Y_n)$$

and

$$s' = s(X_1^{dv}, X_2, ..., X_m, Y_1^{eu}, Y_2, ..., Y_n)$$

are non-constant factors of

$$q' = P(f(X_1^{dv}, X_2, ..., X_m), g(Y_1^{eu}, Y_2, ..., Y_n)$$

such that $(r', s') = (1)$. If $dv = 1$ or $eu = 1$, q is linear and unitary in Y_1 or in X_1, whence the assertion follows trivially. Otherwise, the degree form of q' is

$$aX_1^{deuv} + bY_1^{deuv} \qquad \text{with} \quad a, b \in k^x,$$

which is squarefree, as $p \nmid deuv$. But this contradicts the proposition and proves $(r, s) \neq (1)$.

(b) Assume that $P(f(\mathbf{X}), g(\mathbf{Y}))$ is reducible. Then by [5] there are polynomials $F \in k[U]$, $G \in k[V]$, $r \in k[\mathbf{X}]$, $s \in k[\mathbf{Y}]$ such that $f(\mathbf{X}) = F(r(\mathbf{X}))$, $g(\mathbf{Y}) = G(s(\mathbf{Y}))$ and $P(F(U), G(V))$ is reducible. From $\deg F \mid \deg f$ and $\deg G \mid \deg g$ we see that $\gcd(e \cdot \deg F, d \cdot \deg G) = 1$; moreover, by [1], $P(F(U), G(V))$ is a generalized difference polynomial of type $(e \cdot \deg F, d \cdot \deg G)$. So it suffices to prove the assertion of part (b) of Corollary 2. With the notation used there assume that there are non-constant polynomials q_1, q_2 such that

$$P(U, V) = q_1(U, V)\, q_2(U, V). \tag{1}$$

This implies

$$P(U^d, V^e) = q_1(U^d, V^e)\, q_2(U^d, V^e). \tag{2}$$

Now let Q_i be the degree form of $q_i(U^d, V^e)$ $(i = 1, 2)$. Looking at the degree form in (2), we obtain an equation

$$aU^{de} + bV^{de} = Q_1 Q_2 \qquad \text{with} \quad a, b \in k^x. \tag{3}$$

If $e = 1$, P is linear in U; i.e., P is irreducible. Now let $e > 1$. Then by (3), there is a monomial of the form U^{du}, $0 < u < e$, occurring in Q_1. If $U^{di}V^{ej}$, $i, j \geqslant 0$, is any monomial which occurs in Q_1, we have

$$di + ej = du \qquad \text{and} \qquad i \leqslant u < e. \tag{4}$$

As $gcd(d, e) = 1$, (4) implies $u = i$ and $j = 0$, i.e., $Q_1 = cU^{du}$ for some $c \in k^x$. This is a contradiction to (3), which finishes the proof.

References

1. S. Abhyankar and L. A. Rubel, Every difference polynomial has a connected zero-set, *J. Indian ath. Soc.* **43** (1979), 69–78.
2. A. Ehrenfeucht, Kryterium absolutnej nierozkladalnosci wielomianow, *Prace Math.* **2** (1958), 167–169.
3. L. Panitopol and D. Ştefănescu, Some criteria for irreducibility of polynomials, *Bull. Math. Soc. Sci. Math. R. S. Roumanie (N. S.)* **29** (1985), 69–74.
4. L. A. Rubel, A. Schinzel, and H. Tverberg, On difference polynomials and hereditarily irreducible polynomials, *J. Number Theory* **12** (1980), 230–235.
5. A. Schinzel, Reducibility of polynomials in several variables, *Bull. Acad. Polon. Sci. Ser. Sci. Math. Aster. Phys.* **11** (1963), 633–638.
6. H. Tverberg, A remark on Ehrenfeucht's criterion for irreducibility of polynomials, *Prace Mat.* **18** (1964), 117–118.